# INFORMATION SERVER DEVICE EQUIPPED WITH CIPHERING PROCESSING FUNCTION

**Publication number:** JP2002182560
**Publication date:** 2002-06-26
**Inventor:** SATO MIKIKO; OKAZAWA KOICHI
**Applicant:** HITACHI LTD
**Classification:**
**- international:** ***G06F21/20; G06F9/46; G06F15/00; G09C1/00; H04L9/08;*** **G06F21/20; G06F9/46; G06F15/00; G09C1/00; H04L9/08;** (IPC1-7): G09C1/00; G06F9/46; G06F15/00; H04L9/08
**- European:**
**Application number:** JP20000383117 20001212
**Priority number(s):** JP20000383117 20001212



Abstract of **JP2002182560**

PROBLEM TO BE SOLVED: To provide a means for preventing a secret key from leaking and a means for reallocating computer resources of an information server device according to the busyness of processing for cipher communication and non-cipher communication while evading a decrease in the response speed of the information server device due to cipher processing. SOLUTION: A normal OS which logically divides the computer resources of the information server device and administers the transmission and reception of information and a secure OS which administers a function of deciphering a ciphertext ciphered with an open key at a request from the normal OS are placed in operation. Further, the device is provided with a means which measures information on the CPU use rates of the secure OS and normal OS and information on the memory use rates, informs a system administrator of the computer resource use state of the information server device when a set threshold is exceeded, and allows the system administrator having been informed to reallocate the computer resources of the information server device.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－182560
（P2002－182560A）
(43)公開日　平成14年６月26日(2002.6.26)

| (51)Int.Cl.⁷ | | 識別記号 | FI | | テーマコード*(参考) |
|---|---|---|---|---|---|
| G09C | 1/00 | 620 | G09C | 1/00 | 620Z 5B085 |
| G06F | 9/46 | 350 | G06F | 9/46 | 350 5B098 |
| | 15/00 | 330 | | 15/00 | 330A 5J104 |
| H04L | 9/08 | | H04L | 9/00 | 601A |
| | | | | | 601E |

審査請求　未請求　請求項の数21　ＯＬ　（全 18 頁）

(21)出願番号　特願2000－383117(P2000－383117)

(22)出願日　平成12年12月12日(2000.12.12)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　佐藤　未来子
神奈川県海老名市下今泉810番地　株式会社日立製作所インターネットプラットフォーム事業部内

(72)発明者　岡澤　宏一
神奈川県海老名市下今泉810番地　株式会社日立製作所インターネットプラットフォーム事業部内

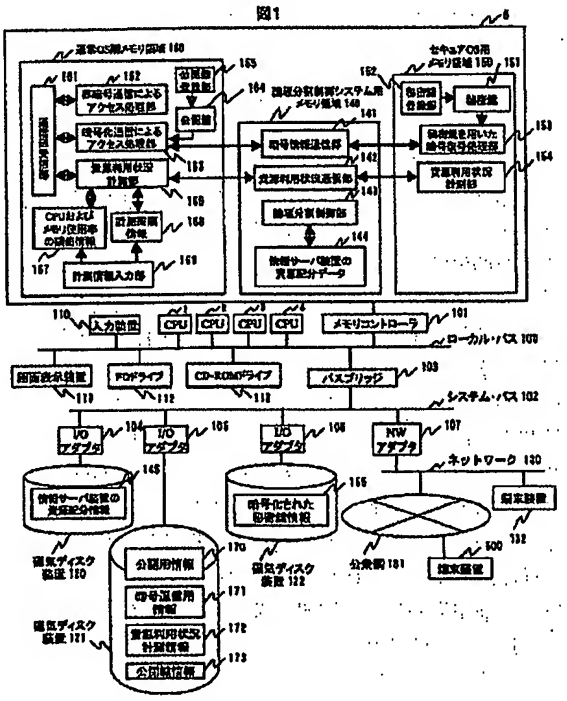
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　暗号処理機能を備えた情報サーバ装置

(57)【要約】
【課題】暗号処理による情報サーバ装置の反応速度低下を回避しつつ、秘密鍵の漏洩を防ぐ手段、および、情報サーバ装置の計算機資源を、暗号通信、非暗号通信の処理の忙しさに応じて再配分するための手段を提供することである。
【解決手段】情報サーバ装置の計算機資源を論理的に分割し、情報の送受信を司る通常ＯＳと、通常ＯＳからの依頼に基づき、公開鍵で暗号化された暗号文を復号処理する機能を司るセキュアＯＳとを稼動させる。また、セキュアＯＳおよび通常ＯＳのＣＰＵ使用率の情報と、メモリ使用率の情報とを計測し、設定した閾値を超えた場合に、システム管理者に情報サーバ装置の計算機資源使用状況を通知し、前記通知を受けたシステム管理者が情報サーバ装置の計算機資源を再配分する手段を設ける。

図1



【特許請求の範囲】

【請求項１】ネットワーク上の端末装置との間で公開鍵暗号方式を用いた通信を行う、情報サーバ装置における公開鍵暗号処理の負荷分散方法において、前記端末装置に配布される公開鍵に対応する秘密鍵を、前記情報サーバ装置で実行される暗号処理プログラムの専有するメモリ領域に保持するステップと、前記端末装置により前記公開鍵を用いて暗号化され、前記情報サーバ装置にネットワークを介して送信された情報を受信した前記情報サーバ装置で実行される他のプログラムから、前記暗号化された情報とその復号化依頼を前記暗号処理プログラムにより受信するステップと、前記公開鍵を用いて暗号化された情報を、前記秘密鍵を用いて前記暗号処理プログラムにより復号化するステップと、前記暗号処理プログラムから前記復号化を依頼した前記他のプログラムへ、前記復号化した情報を返信するステップと、を有することを特徴とする公開鍵暗号処理方法。

【請求項２】前記公開鍵で暗号化される情報が、前記端末装置と前記情報サーバ装置の間の共通鍵暗号方式による通信で用いられる共通鍵であることを特徴とする請求項１に記載の公開鍵暗号処理方法。

【請求項３】前記暗号処理プログラムは、前記情報サーバ装置上で実行される前記他のプログラムとのみ通信を行うことを特徴とする請求項１に記載の公開鍵暗号処理方法。

【請求項４】前記暗号処理プログラム及び前記他のプログラムが使用するＣＰＵとメモリの使用率をそれぞれ計測するステップと、前記暗号処理プログラムと前記他のプログラムのそれぞれに対しあらかじめ決定された前記ＣＰＵと前記メモリの使用率の閾値を保持するステップと、前記暗号処理プログラムと前記他のプログラムのそれぞれについて、計測された前記使用率と前記閾値を比較することで前記使用率が前記閾値を越えたかを監視するステップと、前記使用率が前記閾値を越えていた場合に、前記暗号処理プログラムと前記他のプログラムが使用する前記ＣＰＵと前記メモリの使用率の再配分を行うステップと、を有することを特徴とする、請求項１に記載の公開鍵暗号処理方法。

【請求項５】ネットワーク上の端末装置が公開鍵で暗号化した情報をネットワークを介して受け取り、前記公開鍵に対応する秘密鍵を用いて複合化する情報サーバ装置において、前記端末装置から送信された前記暗号化した情報を受信した他のプログラムから、前記暗号化した情報およびその復号化依頼を受け取り、前記公開鍵に対応する秘密鍵を前記他のプログラムの読み書きが許可されていないメモリ領域に保持し、前記復号化依頼を受信して前記暗号化された情報の復号化を前記秘密鍵を用いて行い、前記復号化した情報を送信元の前記他のプログラムに返信する暗号処理プログラムが稼動することを特徴とする情報サーバ装置。



【請求項６】前記公開鍵で暗号化される情報が、ネットワーク上の端末装置と前記情報サーバ装置の間で行われる共通鍵暗号方式の通信に用いる共通鍵であることを特徴とする請求項５に記載の情報サーバ装置。

【請求項７】前記暗号処理プログラムが情報の送受信を行う対象は、前記他のプログラムのみであることを特徴とする請求項５に記載の情報サーバ装置。

【請求項８】前記暗号処理プログラムは、ネットワーク上に情報を送出しネットワーク上の情報を受信するネットワーク通信機能を持たないことを特徴とする請求項５に記載の情報サーバ装置。

【請求項９】前記情報サーバ装置上で稼動する各プログラムが、前記各プログラムが使用するＣＰＵ及びメモリの資源使用率を所定の時間毎に計測する手段と、計測された前記資源使用率の情報を保持する手段と、計測された前記資源使用率を前記情報サーバ装置の出力装置に出力する手段と、を有することを特徴とする請求項５に記載の情報サーバ装置。

【請求項１０】計測される前記資源使用率に対する閾値を入力する手段と、入力された前記閾値を保持する手段と、前記ＣＰＵ及び前記メモリの資源使用率を設定する手段と、を有することを特徴とする請求項９に記載の情報サーバ装置。

【請求項１１】計測された前記資源使用率と前記閾値を比較し、計測された前記資源使用率が前記閾値を越えたかを監視する手段と、計測された前記資源使用率が前記閾値を越えた場合に、計測された前記資源使用率及び、前記閾値を越えた事を前記出力装置に出力し、各プログラムに対する計算機資源の再配分を行う手段を有することを特徴とする請求項１０に記載の情報サーバ装置。

【請求項１２】論理分割制御システムにより、前記情報サーバ装置が有する計算機資源のうち少なくともＣＰＵ及びメモリを各プログラムに対し配分する手段及びそのための入力装置と、各プログラムに対する前記計算機資源の分配の状況を出力する手段及びそのための出力装置を有することを特徴とする請求項５に記載の情報サーバ装置。

【請求項１３】前記出力装置に、論理分割制御システムにより分割された前記計算機資源の各論理分割単位ごとに前記論理分割単位を識別するための情報、前記論理分割単位の名称、少なくとも前記論理分割単位が使用する前記ＣＰＵ使用率及び前記論理分割単位が使用する前記メモリの容量、前記論理分割単位のＯＳ起動用のデバイスを識別するための情報、前記論理分割単位が使用する割り込み要求番号、前記論理分割単位の種別ごとの、割り当てられた前記メモリの容量、未使用の前記メモリの容量、を出力する第一の出力手段と、前記計算機資源の再配分を行うために前記入力装置から入力された、前記論理分割単位の名称、少なくとも前記論理分割単位にこれから使用させる前記ＣＰＵの使用率及び前記論理分割

単位にこれから使用させる前記メモリ容量、を前記出力装置に出力する第二の出力手段と、を有することを特徴とする請求項１２に記載の情報サーバ装置。

【請求項１４】ネットワーク上の端末装置との間で公開鍵暗号方式を用いた通信を行う情報サーバ装置で実行される少なくとも一つのプログラムを記録したプログラム記録媒体において、前記少なくとも一つのプログラムが、前記端末装置に配布される公開鍵に対応する秘密鍵を、前記情報サーバ装置で実行される前記少なくとも一つのプログラムにより専有されるメモリ領域に保持するステップと、前記端末装置から前記情報サーバ装置へ送信された前記公開鍵で暗号化された情報を、前記情報サーバ装置上で実行される他のプログラムを介して受け取るステップと、前記秘密鍵を用いて前記他のプログラムから受け取った情報の復号化を行うステップと、前記復号化した情報を前記他のプログラムに返信するステップと、を有するプログラムであることを特徴とするプログラム記録媒体。

【請求項１５】少なくとも論理的に分割されたＣＰＵ及びメモリ領域と、ネットワークに対し情報の送受信を行うネットワーク接続装置を場合により割り当てられ、その上で少なくとも一つ以上のプログラムが実行される仮想計算機を、少なくとも二台以上有する情報サーバ装置において、一つの前記仮想計算機上で実行される暗号処理プログラムが、前記暗号処理プログラムが実行される前記仮想計算機とは異なる他の、前記ネットワーク接続装置を割り当てられた前記仮想計算機で実行されるプログラムにより受信された、ネットワーク上の端末装置により公開鍵を用いて暗号化された情報を、前記公開鍵に対応する秘密鍵を用いて復号化することを特徴とする情報サーバ装置。

【請求項１６】前記秘密鍵は前記暗号処理プログラムが専有するメモリ領域に保持されることを特徴とする請求項１５に記載の情報サーバ装置。

【請求項１７】前記仮想計算機に割り当てられた前記ＣＰＵ又は前記メモリ領域もしくはその両方について前記仮想計算機ごとに使用状況を計測し、前記使用状況に対するあらかじめ設定された閾値と比較し、前記閾値を超えた前記仮想計算機の前記ＣＰＵ又は前記メモリ領域の使用量を増加せしめる手段を有することを特徴とする請求項１５に記載の情報サーバ装置。

【請求項１８】ネットワーク上の端末装置が公開鍵で暗号化した情報をネットワークを介して受け取り、前記公開鍵に対応する秘密鍵を用いて複合化する情報サーバ装置において、前記情報サーバ装置の少なくともＣＰＵ及びメモリ領域が論理的に分割され、分割された前記ＣＰＵ及びメモリ領域ごとに、一つ以上のプログラムを実行する仮想計算機が少なくとも二つ以上稼動する前記情報サーバ装置であって、前記仮想計算機のうちの少なくとも一つの仮想計算機が、前記端末装置から送信された前記暗号化した情報を受信した、前記少なくとも一つの仮想計算機とは異なる他の仮想計算機が実行する他のプログラムから、前記暗号化した情報およびその復号化依頼を受け取り、前記公開鍵に対応する秘密鍵を専有するメモリ領域に保持し、前記復号化依頼を受信して前記暗号化された情報の復号化を前記秘密鍵を用いて行い、前記復号化した情報を送信元の前記他のプログラムに返信する暗号処理プログラムを実行することを特徴とする情報サーバ装置。

【請求項１９】前記暗号処理プログラムが稼動する仮想計算機は、ネットワークに対し情報の送受信を行うネットワーク通信機能を持たないことを特徴とする請求項１８に記載の情報サーバ装置。

【請求項２０】前記仮想計算機に割り当てられた論理的な前記ＣＰＵ及び前記メモリ領域の使用状況を、前記仮想計算機ごとに計測し、計測した前記使用状況とあらかじめ設定された前記使用状況を比較し、計測した前記使用状況があらかじめ設定された前記使用状況を超えている場合は、前記仮想計算機が使用する前記ＣＰＵもしくは前記メモリ領域又はその両方の使用量を増加させることを特徴とする請求項１８に記載の情報サーバ装置。

【請求項２１】前記仮想計算機間の通信は、前記少なくとも一つの仮想計算機が専有する前記メモリ領域に通信を行うデータを格納し、前記他の仮想計算機が、前記第1の仮想計算機が専有する前記メモリ領域から前記データを取得することで行われることを特徴とする請求項１８に記載の情報サーバ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークに接続された端末装置と情報サーバ装置間で公開鍵暗号方式を用いて機密度の高い情報を通信する際に、情報サーバ装置で行う公開鍵暗号方式の復号化処理の負荷を、情報サーバ装置で備える計算機資源を有効に活用することで軽減する方法に関する発明である。

【０００２】

【従来の技術】インターネットに接続された、一般的なＷｅｂクライアントであるパーソナル・コンピュータやＡＴＭ（Ａｕｔｏｍａｔｉｃ　Ｔｅｌｌｅｒ　Ｍａｃｈｉｎｅ）、カードリーダ等の個人認識を行うための入力装置を場合により持つコンピュータ等の端末装置は、Ｗｅｂサーバに代表される、インターネットに接続された情報サーバ装置と通信し、所望の情報の取得や送付を行う。

【０００３】今日のインターネットでは、サーバに掲載する情報の取得という目的以外に、インターネットを利用した商品注文や、銀行取引、株の売買といったことが可能となっている。このような流通を行ったり金融情報を掲載しているサイトに対して、端末装置を操作するユーザが、ユーザの個人情報、クレジットカード番号、暗

証番号といった他人には知られたくない情報を、インターネットを経由して送信する必要がある。従来、他人に知られても良い一般的な情報に関しては、暗号化されていない平文が送受信されるが、前述したような機密情報に関しては、安全な送受信を行うために「ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）」という暗号通信を使うのが一般的である。

【０００４】ＳＳＬでは、現在普及している公開鍵暗号方式が用いられる。公開鍵暗号方式とは、秘密鍵と公開鍵と呼ばれる２つの種類の鍵を用いて、一方の鍵で暗号化した情報を、他方の鍵で復号化するといった暗号方式である。公開鍵暗号方式で使われる鍵は、一方向関数と呼ばれる数学的な計算手順で決められるものなので、片方の鍵（公開鍵）が分かっても、もう片方の鍵（秘密鍵）を解読することはほぼ不可能としている。

【０００５】また、公開鍵暗号方式は、従来の共通鍵暗号方式（お互いに共通の暗号鍵を持ち、暗号情報の送受信を行うもの）に比べ、暗号処理の計算量が増大することが知られている。一方で、公開鍵暗号方式は，従来の共通鍵暗号方式に比べて，公開鍵は秘匿する必要がないので鍵の配布が容易であり、インターネットでの暗号通信に適した方式である。またＳＳＬは、前記各々の暗号方式の利点を活かした暗号通信手順となっている。すなわち、実際に端末装置と情報サーバ間で交換する機密情報の送受信には、計算処理量が軽い共通鍵暗号方式を用い、その共通鍵暗号方式に用いる共通鍵の送受信に公開鍵暗号方式を用いる、という通信方式となっている。

【０００６】尚、ＳＳＬについては、日経インターネットテクノロジー特別付録「ＥＣ時代のＷｅｂシステム高速化」（日経ＢＰ社、２０００年１２月号、ｐ３３～ｐ３５）に詳しい。

【０００７】しかし、この公開鍵暗号方式を処理する情報サーバ装置のＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）は、公開鍵暗号方式の復号化処理に多くの時間を必要とし、また復号化処理を速く行うには多くのメモリ容量が必要であり、情報サーバ装置の負荷が増大することが知られている。このことにより、例えば、ＳＳＬ通信機能を持つ情報サーバ装置に対し、ＳＳＬ通信を行う複数の端末装置から同時に多数のアクセス要求が発生した場合、情報サーバ装置から端末装置への応答速度が極端に低下してしまう、という問題が発生する。

【０００８】現状では、以下の方法で、情報サーバ装置への公開鍵暗号処理による負荷を軽減している。

【０００９】（１）サーバを複数台設ける方法
非暗号通信によるアクセスを受け付ける情報サーバ装置と、暗号通信によるアクセスを受け付ける情報サーバ装置とを別々に設ける。これらの情報サーバ装置は、端末装置を利用するユーザからはどちらの情報サーバ装置とも通信可能となるよう、ネットワークに接続されている。

【００１０】（２）アクセラレータ装置を導入する方法
暗号処理専用のアクセラレータ装置を情報サーバ装置に接続し、暗号処理をアクセラレータ装置で行い、本来の情報サーバ装置の処理、すなわち、端末装置との情報送受信、受信情報の処理、送信情報の作成等にＣＰＵを使用する。

【００１１】しかしながら、これらの方法にはそれぞれ問題点がある。

【００１２】（１）サーバを複数設ける方法の問題点
公開鍵暗号方式を処理する情報サーバ装置では、一般的に、秘密鍵の情報を暗号化して、磁気ディスク等の記憶装置内に機密保管しておく。復号処理に秘密鍵を用いる際に、特定のパスフェーズを入力しなければ、秘密鍵を使用するアプリケーションから読み取れない仕組みがほどこされている。そして、パスフェーズが入力されれば、情報サーバ装置のメモリ内に秘密鍵の情報がロードされ、暗号の復号処理に用いられる。

【００１３】通常のＯＳ（オペレーティングシステム）では、障害発生時に、メモリに保持されている全ての情報を、磁気ディスク装置へ格納する手段がとられる（メモリダンプと呼ばれる）。これは、サーバ装置を、障害発生前の状態に復帰させたり、または、障害発生の原因究明に利用するために行われる。

【００１４】もし、メモリ上に秘密鍵の情報が保持されている時に障害が発生し（あるいは、故意に障害を発生させられ）、メモリダンプが生成されれば、秘密鍵の情報は暗号化されない状態で磁気ディスク装置へ格納される可能性がある。

【００１５】そして、このような情報サーバ装置がネットワークに接続され、遠隔より障害復旧等の作業をする場合、ネットワークに接続された他の端末装置から、磁気ディスク装置やメモリ内の情報を読み取られる可能性がないとは言えない。

【００１６】（２）アクセラレータ装置を導入する方法の問題点
アクセラレータ装置では、秘密鍵をアクセラレータ内の不揮発性メモリ内に登録し厳重に保管する機能を設けており、情報サーバ装置のメモリ上、および、情報サーバ装置に付属する磁気ディスク装置上には秘密鍵を置かずに、暗号処理する仕組みとなっている。そのため、秘密鍵の漏洩をほぼ完全に防ぐことが可能である。

【００１７】しかし、そういった機能をもつアクセラレータ装置1台の価格は、一般の情報サーバ装置1台分の価格にほぼ相当するものもあり、大変高価である。この大きな投資をしたアクセラレータ装置は暗号処理専用機器なので、暗号処理が頻繁に行われない時間が存在しても、その間にアクセラレータ装置内に備え付けられているＣＰＵやメモリなどの資源を他の目的に使用することはできない。

【００１８】以上の問題点の他に、以下の問題点も残されている。情報サーバ装置の暗号通信と非暗号通信がどの位の割合で発生するものかは、情報サーバ装置に掲載する情報（すなわち、一般に公開する情報）、あるいは、時刻によっても変動するものであり、一概に予測できるものではない。

【００１９】サーバを複数設ける方法、あるいは、アクセラレータ装置を導入する方法の場合、ある程度、暗号および非暗号通信の変動を予想して情報サーバ装置のシステム構成を考える必要がある。そして、一度決定したシステム構成を、安易に変更することはできない。

【００２０】

【発明が解決しようとする課題】このように従来の技術では、公開鍵暗号方式による通信を行う情報サーバ装置において、秘密鍵を用いた復号化処理の負荷が高くなった場合に、その他の処理を行う負荷の小さなＣＰＵや使用されていないメモリ等の計算機資源を、復号化処理のために使用することが容易では無かった。また復号化処理専用の処理装置を用意しても、その装置のＣＰＵやメモリを他の用途に使用することができず、計算機資源の有効利用をすることができなかった。

【００２１】また従来の技術では、情報サーバ装置が保持する秘密鍵の秘匿性が低下する場合が存在する。

【００２２】

【課題を解決するための手段】そこで上記課題を解決するために本発明では、以下に説明する公開鍵暗号処理の負荷分散方法、及びこの方法を用いた情報サーバ装置を提供する。

【００２３】本発明の、ネットワーク上の端末装置との間で公開鍵暗号方式を用いた通信を行う情報サーバ装置上では、稼動する複数のプログラムのうちの一つである暗号処理プログラムが秘密鍵の保持及びこの秘密鍵を用いた情報の復号化を一手に処理するよう設定される。情報サーバ装置と端末装置間における、ネットワークを介した情報の送受信処理は、暗号処理プログラム以外の、ネットワーク接続装置を制御する他のプログラムが行う。他のプログラムが受信した情報が公開鍵で暗号化された情報であった場合は、暗号処理プログラムに受信した情報の復号化を依頼する。そして暗号処理プログラムは情報を復号化すると、復号化依頼をした他のプログラムに復号化した情報を返送し、その後のこの情報に関する処理は他のプログラムにて行われる。

【００２４】復号化処理を行う暗号処理プログラムがネットワーク通信機能を持たない、つまりネットワーク接続装置を用いたネットワーク上の端末装置との通信を直接に行わないよう設定されていれば、ネットワーク上の端末装置やその他機器は、ネットワーク接続装置を制御する他のプログラムを介して暗号処理プログラムにアクセスすることとなる。つまり、ネットワーク上の第三者が暗号処理プログラムに直接アクセスすることはできず、暗号処理プログラムが秘密鍵を専有するため秘密鍵の機密性は高まり、秘密鍵の情報漏洩を防ぐことができる。さらに障害発生時に、暗号処理プログラムがメモリダンプ情報を生成しないように設定されていれば、秘密鍵の情報漏洩の防止効果をさらに高めることができる。

【００２５】また、秘密鍵を用いた復号化処理を行う暗号処理プログラムと、その他のプログラムについて、各々のプログラムが用いるＣＰＵやメモリ等の計算機資源の使用率等の使用状況を所定の時間毎、つまり装置の管理者等に設定された時間間隔ごとに計測し、この計測された使用状況が所定の値に達した場合に計算機資源の再配分を行うことで、暗号処理とその他処理の負荷の変動に応じた計算機資源の有効活用を行うことができる。

【００２６】

【発明の実施の形態】本発明の一実施形態を、図面を参照して以下に説明する。図１に、本実施形態の情報サーバ装置の構成図を示す。情報サーバ装置にはローカル・バス１００を設け、当該情報サーバの各種処理を実行するＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１～４と、種々の情報を格納するメモリ５を接続するためのメモリコントローラ１０１と、情報サーバ装置に各種情報を入力するキーボードやマウス等の入力装置１１０と、出力装置として情報サーバ装置の各種情報を表示するモニタ等の画面表示装置１１１と、ＦＤ（Ｆｌｏｐｐｙ Ｄｉｓｋ）に対して情報を読み書きするＦＤドライブ１１２と、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｋ ＲＯＭ）に対して情報を読み書きするＣＤ－ＲＯＭドライブ１１３と、各種入出力装置を接続するためのシステム・バス１０２とローカル・バス１００とを接続し制御するバスブリッジ１０３を備える。システム・バス１０２には、前記バスブリッジ１０３の他に、磁気ディスク装置等の外部記憶装置１２０～１２２を接続するためのＩ／Ｏアダプタ１０４～１０６と、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）等のネットワーク１３０を接続するためのネットワーク接続装置である、ネットワーク用アダプタ１０７を備える。これら計算機資源は後述する論理分割制御システムにより分割され、それらＣＰＵやメモリ領域、その他記憶装置等の一部ずつが論理分割単位としてまとめられ、この論理分割単位の計算機資源を使用して仮想計算機が稼動し、その上でＯＳが実行される。この後の説明に用いる通常ＯＳとセキュアＯＳは、それぞれ異なる仮想計算機上で実行されるＯＳである。

【００２７】本実施形態では、ＣＰＵの数を４つとしているが、情報サーバ装置のＣＰＵがこれ以下であったり、もしくはこれ以上のＣＰＵを有していても良い。また、出力装置としてモニタ等の画面表示装置を例示したが、この他にプリンタ等の印刷機械が接続されて、情報サーバ装置の各種情報が紙面に印刷されても良い。また、携帯性に優れた情報記録媒体を用いるための装置と

して、前述のＦＤドライブやＣＤ－ＲＯＭドライブの他にＤＶＤ－ＲＡＭ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ　ＲＡＭ）ドライブやＭＯ（Ｍａｇｎｅｔｏ　Ｏｐｔｉｃａｌ）ドライブのような、その他の携帯性に優れた情報記録媒体用の装置が接続されていてもよい。また、図１において、ネットワーク用アダプタを一つのみ図示しているが、複数のネットワーク用アダプタがシステム・バスに接続されていてもよい。

【００２８】ネットワーク１３０は、例えば、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等の公衆網１３１に接続されており、情報サーバ装置は、公衆網１３１およびネットワーク１３０を経由して、公衆網１３１に接続された任意の端末装置５００と通信する。また、ネットワーク１３０には、本情報サーバ装置からの資源再配分要求を受信するための端末装置１３２が接続されている。

【００２９】システム管理者は、入力装置１１０や画面表示装置１１１を用いて、情報サーバ装置の資源配分を行うことができるが、端末装置１３２を用いて情報サーバ装置の資源配分の決定等を行うこともでき、この場合は資源配分に必要な情報が出力される出力装置は情報端末１３２のモニタ等となる。以下、システム管理者は端末装置１３２を介して情報サーバ装置からの資源配分要求を受け、実際の作業は場所を移動して入力装置１１０と画面表示装置１１１を用いて行うこととして実施例を示す。

【００３０】メモリ５上には、情報サーバ装置の計算機資源を論理分割するシステム用のメモリ領域１４０と、暗号処理を司るセキュアＯＳ用メモリ領域１５０と、端末装置５００からのアクセス要求に応えたり、情報サーバ装置の資源利用状況を計測する処理を司る通常ＯＳ用メモリ領域１６０とを備える。本実施例では、秘密鍵を保持しそれを用いた情報の復号処理を行う暗号処理プログラムがセキュアＯＳに、他のプログラムが通常ＯＳに相当する。

【００３１】本発明における情報サーバ装置の計算機資源を論理的に分割し、各計算機資源上でＯＳを実行させ、それらＯＳ間の通信を仲介するシステム・プログラムである論理分割制御システムが使用する、論理分割制御システム用メモリ領域１４０は、通常ＯＳとセキュアＯＳ間の暗号情報の通信を司る暗号情報通信部１４１と、通常ＯＳとセキュアＯＳ間で資源利用状況に関する情報の通信を司る資源利用状況通信部１４２と、情報サーバ装置の計算機資源を論理的に分割する処理を司る論理分割制御部１４３と、論理分割制御部１４３から参照する現状配分されている計算機資源の配分情報を納めるメモリ領域１４４とを有する。

【００３２】通常ＯＳとセキュアＯＳは、論理分割制御システムが提供する暗号情報通信部１４１や資源利用状況通信部１４２を介して通信を行う。この仮想計算機間の通信は様々な方法で実行することができ、例えば共有ディスクを用意して各仮想計算機がそれに対しアクセスを行う方法や、物理的に通信インタフェースを設けこのインタフェースを介して通信を行う方法がある。

【００３３】又、通常ＯＳ、セキュアＯＳがそれぞれ有するメモリ領域を介した通信も考えられる。このメモリ領域を介した通信を行うには、情報サーバ装置を起動する時に、通常ＯＳ用メモリ領域１６０に仮想計算機間通信用のメモリ領域を確保し、同じくセキュアＯＳ用メモリ領域にも仮想計算機間通信用のメモリ領域を確保する。通常ＯＳからセキュアＯＳにデータを送信する場合は、まず通常ＯＳがその仮想計算機間通信用のメモリ領域にデータを格納する。そして通常ＯＳは、データが格納されているメモリ領域の先頭アドレスやデータのサイズ、通信相手（この場合はセキュアＯＳ）等を目的に応じて論理分割制御システムの暗号情報通信部１４１もしくは資源利用状況通知部１４２に通知する。通知を受けた論理分割制御システムの暗号情報通信部１４１や資源利用状況通知部１４２といったＯＳ間通信用プログラムは、通信相手をセキュアＯＳと識別したら、このセキュアＯＳが稼動する仮想計算機に対し割り込み要求を通知する。この割り込み要求に対する応答を受けたＯＳ間通信用プログラムは、先に通常ＯＳから受信した、データが格納された先頭アドレスやデータのサイズ等の情報をセキュアＯＳに通知し、そのメモリ領域からセキュアＯＳのメモリ領域にデータを格納する処理を行うよう要求する。セキュアＯＳはこの要求を受け、そのデータを格納するため確保したセキュアＯＳ用メモリ領域の一部にデータを格納する。

【００３４】セキュアＯＳから通常ＯＳへデータを送信する場合も同様であるが、セキュリティを高めるために通常ＯＳがセキュアＯＳ用メモリ領域１５０に一切アクセス出来ないようにするのであれば、論理分割制御システム用メモリ領域１４０の一部にセキュアＯＳが送信を要求するデータを一度格納し、そのデータを通常ＯＳが通常ＯＳ用メモリ領域に格納するようにすれば良い。もしくは、通常ＯＳ用メモリ領域１６０にセキュアＯＳが直接データを格納しても良い。このように、メモリ領域を介して各仮想計算機上のＯＳが通信を行う場合は、論理分割制御システム上のＯＳ間通信用プログラムは、あるＯＳからのメモリ領域へのアクセス要求を通信相手のＯＳに通知するという処理を行う。

【００３５】論理分割制御部１４３は、入力装置１１０からの入力を受け付け、前記資源配分情報１４４を更新したり、更新した情報に基づいて、本情報サーバ装置上で稼動する仮想計算機が使用する計算機資源を配分し直す機能を備える。また、前記論理分割制御部１４３は、前記資源配分情報１４４が更新された際に、更新された資源配分情報１４４を磁気ディスク装置１２０内の資源配分情報１４５へ格納する機能を持つ。また、本情報サ

ーバ装置に電源を投入した時に、前記資源配分情報１４５の内容の一部を資源配分情報１４４へコピーし、コピーした資源配分情報１４４を参照しながら、本情報サーバ装置を稼動する機能を備える。

【００３６】セキュアＯＳ用メモリ領域１５０はセキュアＯＳが専有するメモリ領域であり、公開鍵暗号の復号化に用いる秘密鍵を入力装置１１０から入力してメモリ領域151に格納し、さらに秘密鍵を暗号化して磁気ディスク装置１２２内の秘密鍵情報１５５へ格納したり、セキュアＯＳ起動時に磁気ディスク装置１２２から暗号化された前記秘密鍵情報１５５を読み出し、入力装置１１０から入力するパスフェーズで復号化し、前記秘密鍵を納めるメモリ領域１５１へ格納する機能を備えた秘密鍵登録部１５２と、秘密鍵を用いた暗号処理を司る暗号復号処理部１５３と、セキュアＯＳの資源利用状況を計測する資源利用状況計測部１５４とを備える。

【００３７】通常ＯＳ用メモリ領域１６０は通常ＯＳが用いるメモリ領域であり、ネットワーク１３０を介して端末装置５００と通信する通信送受信部１６１と、磁気ディスク装置１２１に保持している公開用情報１７０を非暗号通信により端末装置へ提供する処理を司るアクセス処理部１６２と、磁気ディスク装置１２１に保持している暗号通信用情報１７１を暗号化通信により端末装置へ提供する処理を司るアクセス処理部１６３と、アクセス処理部１６３の暗号通信に用いる公開鍵情報を、入力装置１１０から入力し公開鍵のメモリ領域１６４に登録し、さらに磁気ディスク装置１２１内の公開鍵情報１７３へ格納したり、通常ＯＳ起動時に前記公開鍵情報１７３を読み出し公開鍵のメモリ領域１６４へ格納する機能を備えた公開鍵登録部１６５とを備える。

【００３８】また、通常ＯＳ用メモリ領域１６０では、通常ＯＳの処理の忙しさを計測する資源利用状況計測部１６６と、前記資源利用状況計測部１６６から参照されるＣＰＵおよびメモリ使用率の閾値情報１６７と、計測間隔情報１６８と、前記閾値情報１６７と計測間隔情報１６８を入力装置１１０から入力し登録する計測情報入力部１６９を備える。また、セキュアＯＳ用メモリ領域１５０には、セキュアＯＳの処理の忙しさを計測する資源利用状況計測部１５４が存在する。

【００３９】閾値情報と計測間隔情報については、磁気ディスクにこれら情報を格納する領域を設け、通常ＯＳもしくはセキュアＯＳ起動時に磁気ディスク装置から読み出され、それぞれが閾値情報１６７と計測間隔情報１６８に格納され、またこれら処理を行う閾値・計測間隔情報登録部が通常ＯＳ用メモリ領域１６０に存在してもよい。

【００４０】前記ＣＰＵ使用率とは、割り当てられたＣＰＵの何パーセント（％）を使用してプログラムを実行しているかを示す情報である。また、前記メモリ使用率とは、割り当てられたメモリ容量の何パーセント（％）を使用してプログラムを実行しているかを示す情報である。また、前記閾値情報とは、通常ＯＳおよびセキュアＯＳのＣＰＵ資源の使用率、および、メモリ資源の使用率の使用限界、すなわち、処理をこなすために必要な計算機資源が不足したことを示す閾値もしくは境界値である。また、計測間隔情報とは、前記ＣＰＵ使用率とメモリ使用率を計測する間隔を示す情報である。システム管理者は、閾値情報および計測間隔情報を、情報サーバ装置の稼動中いつでも計測情報入力部１６９より入力し更新することが可能であるとする。

【００４１】図２に、本実施例の情報サーバ装置における公開鍵暗号処理の処理手続きの流れを、ＳＳＬの通信手順を用いて端末装置５００と通信する例で説明する。

【００４２】情報サーバ装置の通常ＯＳの暗号化通信によるアクセス処理部１６３は、セキュアＯＳの秘密鍵を用いた暗号復号処理部１５３と暗号情報をやり取りするため、論理分割制御システムの暗号情報通信部１４１に対して経路確保を要求する（ステップ２００）。一方のセキュアＯＳの暗号復号処理部１５３も、暗号情報通信部１４１に対して経路確保を要求する（ステップ２２０）。この経路確保とは、先に説明したメモリ領域を用いたＯＳ間の通信の場合は、通信に用いるメモリ領域を論理分割制御システムに対しあらかじめ通知する処理等である。

【００４３】暗号化通信によるアクセス処理部１６３は、その後、端末装置５００から公開鍵暗号通信開始要求５２０を受け付ける（ステップ２０１）。アクセス処理部１６３は、端末装置５００へ公開鍵情報５２１を送付する（ステップ２０２）。アクセス処理部１６３は、端末装置５００から暗号化情報５２２を受け取り（ステップ２０３）、受信した暗号化情報５２２を、暗号情報通信部１４１を介してセキュアＯＳの復号化処理部１５３へ送付する（ステップ２０４）。暗号復号処理部１５３は、暗号化通信によるアクセス処理部１６３からの復号依頼を受け付け（ステップ２２１）、秘密鍵１５１を使って、暗号化された情報を復号処理し（ステップ２２２）、復号した情報を、暗号情報通信部１４１を介して通常ＯＳのアクセス処理部１６３へ送付する（ステップ２２３）。アクセス処理部１６３は、復号化された情報を受信し（ステップ２０５）、復号化した情報から共通鍵に関する情報を取り出す（ステップ２０６）。前記ステップ２０６で取り出した共通鍵を用いて、情報サーバ装置から送付する情報を暗号化し、返信する情報５２３を作成し（ステップ２０７）、端末装置５００へ送付する（ステップ２０８）。アクセス処理部１６３は、端末装置５００から共通鍵で暗号化された情報５２４を必要に応じて受け取り（ステップ２０９）、共通鍵を用いて復号化し、処理する（ステップ２１０）。そして、前記復号化した情報に応じて、端末装置５００へ返信する情報を作成する（ステップ２０７）。

【００４４】図3に、本実施例の情報サーバ装置における資源利用状況の計測処理の流れを示す。情報サーバ装置の通常ＯＳの資源利用状況計測部１６６は、セキュアＯＳの資源利用状況計測部１５４と資源利用状況に関する情報をやり取りするため、論理分割制御システムの資源利用状況通信部１４２に対して経路確保を要求する（ステップ３００）。一方のセキュアＯＳの資源利用状況計測部１５４も、資源利用状況通信部１４２に対して経路確保を要求する（ステップ３２０）。資源利用状況計測部１６６は、計測情報入力部１６９に対し、閾値情報と計測間隔情報の入力依頼をし、システム管理者から情報入力してもらう（ステップ３１０）。本実施例では、起動時にシステム管理者が閾値情報と計測間隔情報を入力するとしたが、前述のようにこれらの情報をあらかじめ磁気ディスク装置１２１に格納しておき、資源利用状況計測部１６６起動時に磁気ディスク装置１２１内から読み出す方法でもよい。

【００４５】前記ステップ３１０により、閾値情報１６７には、通常ＯＳのＣＰＵ使用率の閾値１６７－１、通常ＯＳのメモリ使用率の閾値１６７－２、セキュアＯＳのＣＰＵ使用率の閾値１６７－３、セキュアＯＳのメモリ使用率の閾値１６７－４という、４つの値が格納される。また、計測間隔情報１６８には、計測間隔の時間情報が格納される。

【００４６】資源利用状況計測部１６６は、計測間隔情報１６８を参照し、次に計測する時刻を現在の時刻から算出し、その時刻になるまで待つ（ステップ３０１）。前記待機する手段としては、一般的に、ＯＳが提供しているタイマー機能を利用する。例えば、通常ＯＳに対し、ある一定の間隔で計測情報入力部１６６の処理を稼動させる、という設定で本発明を実施してもかまわない。

【００４７】次に、資源利用状況計測部１６６は、設定した時刻になると、通常ＯＳでのＣＰＵ使用率、および、メモリ使用率を計測し（ステップ３０２）、セキュアＯＳにＣＰＵ使用率およびメモリ使用率の計測を依頼する（ステップ３０３）。

【００４８】一方、セキュアＯＳの資源利用状況計測部１５４は、通常ＯＳとの通信経路確保３２０の後、通常ＯＳからＣＰＵ使用率およびメモリ使用率の計測依頼が来るのを待ち（ステップ３２１）、計測依頼を受信する（ステップ３２２）。資源利用状況計測部１５４は、セキュアＯＳでのＣＰＵ使用率、および、メモリ使用率を計測し（ステップ３２３）、通常ＯＳへ計測情報を通知し（ステップ３２４）、次の計測依頼を受信するまで待機する（ステップ３２１）。

【００４９】通常ＯＳの資源利用状況計測部１６６は、セキュアＯＳからＣＰＵ使用率の情報、および、メモリ使用率の情報を得る（ステップ３０４）。資源利用状況計測部１６６は、前記資源利用状況の計測情報、すなわち、通常ＯＳのＣＰＵ使用率と、通常ＯＳのメモリ使用率と、セキュアＯＳのＣＰＵ使用率と、セキュアＯＳのメモリ使用率の情報と、計測した日時とを、磁気ディスク装置１２１内の資源利用状況計測情報１７２へ格納する（ステップ３０５）。

【００５０】資源利用状況計測部１６６は、閾値情報１６７を参照し、計測した通常ＯＳとセキュアＯＳそれぞれのＣＰＵ使用率とメモリ使用率の情報が、閾値を超えているかどうかを調べる（ステップ３０６）。

【００５１】具体的には、通常ＯＳのＣＰＵ使用率と閾値情報１６７－１、通常ＯＳのメモリ使用率と閾値情報１６７－２、セキュアＯＳのＣＰＵ使用率と閾値情報１６７－３、セキュアＯＳのメモリ使用率と閾値情報１６７－４とを比較し、計測した使用率の値が閾値を超えたかどうかを確かめる。いずれかの比較においても閾値を超えなかった場合には、ステップ３０１へ進み、計測間隔情報１６８を参照して次の計測時刻を算出し、その時刻になるまで待つ。また、いずれかの比較において、閾値を超えたものがあった場合には、システム管理者に対し、計算機資源の計測結果と、閾値を超えた資源があることを通知する（ステップ３０７）。前記システム管理者は、端末装置１３２を使って、本情報サーバ装置の資源利用状況計測部１６６からの通知を待ちながら、他の仕事をしていてもよい。

【００５２】次に、システム管理者が、情報サーバ装置に対して通常ＯＳとセキュアＯＳに資源を配分し、起動できる状態にする、すなわちインストールの手順と、前記、資源利用状況計測部１６６から何らかの計算機資源が閾値を超えている旨を受信した場合に、計算機の資源を再配分する手順について説明する。再配分の作業は、通知を受けた端末装置１３２からネットワーク１３０を介して行っても良いが、ネットワークのセキュリティが低い場合は、好ましくは前述のとおり入力装置１１０と画面表示装置１１１を用いて直接情報サーバ装置５に入力する方がよい。

【００５３】なお、本実施例の論理分割制御システムには、情報サーバ装置のＣＰＵ資源１～４を本情報サーバ装置で稼動させるＯＳに対し、時分割で共用させる機能を備えているものとする。

【００５４】また、本実施例の情報サーバ装置に備える入出力装置にはそれぞれ、割り込み要求（Ｉｎｔｅｒｒｕｐｔ　Ｒｅｑｕｅｓｔ）番号がわりふられているものとする。前記割り込み要求とは、前記入出力装置が、ＣＰＵの処理中に前記入出力装置の処理を割り込ませるためＣＰＵへ送る要求のことであり、割り込み要求番号とは、その要求がどの入出力装置から送付されたものかを識別するために用いる番号である。本実施例では、磁気ディスク装置１２０の入出力を司るＩ／Ｏアダプタ１０４に、割り込み要求番号「０ｘ０Ｂ」を割り当て、磁気ディスク装置１２１の入出力を司るＩ／Ｏアダプタ１０

５に、割り込み要求番号「０ｘ０Ｃ」を割り当て、磁気ディスク装置１２２の入出力を司るＩ／Ｏアダプタ１０６に、割り込み要求番号「０ｘ０Ｅ」を割り当て、ネットワーク１３０の入出力を司るネットワーク用アダプタ１０７に、割り込み要求番号「０ｘ０Ｄ」を割り当て、前記割り込み要求番号をシステム管理者が認識しているものとする。

【００５５】また、本実施例では、通常ＯＳまたはセキュアＯＳのインストールを行う際に、まずＦＤに格納されている起動用プログラムを用いて起動した後に、通常ＯＳまたはセキュアＯＳのインストール作業を開始するものとする。一般的には、インストールするＯＳに関する情報は、1枚のフロッピー（登録商標）ディスクに納まらないほど情報量が多いため、ＣＤ－ＲＯＭを利用または併用し、ＣＤ－ＲＯＭからＯＳのインストール先、具体的には、磁気ディスク装置のしかるべき位置へ情報をコピーするのが一般的である。本実施例では、フロッピーディスクとＣＤ－ＲＯＭを併用してインストール作業をし、インストール後は、ＯＳを格納した磁気ディスク装置から起動するものとする。

【００５６】図５に、論理分割制御システムの論理分割制御部１４３に対して、入力装置１１０から、通常ＯＳとセキュアＯＳの計算機資源について初期設定する際のコマンド入力画面を示す。前記コマンド入力画面に対する操作は、システム管理者が行うものとする。

【００５７】まず、論理分割制御部１４３に対し、「ｄｅｖｌｉｓｔ」コマンドを入力し（６０１）、情報サーバ装置に接続してあるデバイス、すなわち、ＦＤドライブ１１２と、ＣＤ－ＲＯＭドライブ１１３と、磁気ディスク装置１２０～１２２の一覧を表示させ、情報サーバ装置に接続しているデバイスを識別するための情報としてそれぞれのデバイスに固有に割り振られた番号を得る。本実施例では、ＦＤドライブ１１２のデバイス番号は０１であり（６０２）、1台目の磁気ディスク装置のデバイス番号は８０であり（６０３）、２台目の磁気ディスク装置のデバイス番号は８１であり（６０４）、３台目の磁気ディスク装置のデバイス番号は８２であり（６０５）、ＣＤ－ＲＯＭドライブ１１３のデバイス番号はＦＦである（６０６）。

【００５８】次に、論理分割制御部１４３に対し、通常ＯＳ用の計算機資源を設定する（６０７）。具体的には、「ｓｅｔ」コマンドを入力装置１１０から入力し、そのコマンドの引数として、論理分割単位の名称となる「ｎｏｒｍａｌ－ＯＳ」と（６０８）、最初のＣＰＵ使用比率の割り当てとなる、ＣＰＵ全体の使用率に対する割合「４０」パーセント（％）と（６０９）、通常ＯＳが使用する物理的なメモリ容量「２０４８」メガバイト（ＭＢ）と（６１０）、ＯＳ起動用のデバイスとしてＦＤを使うために、そのＦＤを識別するための情報である、前記手順６０２で調べたＦＤドライブのデバイス番号「０１」と（６１１）、ネットワーク用アダプタ１０７および磁気ディスク装置１２１を利用するために、あらかじめ設定しておいた割り込み要求番号「０ｘ０Ｃ」と「０ｘ０Ｄ」を指定する（６１２）。論理分割制御部１４３は、「ｓｅｔ」コマンドの要求を受け付け、システム管理者が要求した通常ＯＳに割り当てる計算機資源の確保をする。

【００５９】次に、通常ＯＳをインストールする作業をとり行うためのフロッピーディスクをＦＤドライブ１１２へ挿入し、各種通常ＯＳに関する情報を格納してあるＣＤ－ＲＯＭをＣＤ－ＲＯＭドライブ１１３へ挿入する。

【００６０】次に、論理分割制御部１４３に対し、通常ＯＳの計算機資源を実際に使用可能な状況にするために、「ａｃｔｉｖａｔｅ」コマンドを入力する（６１３）。具体的には、「ａｃｔｉｖａｔｅ」コマンドを入力装置１１０から入力し、そのコマンドの引数として、通常ＯＳの論理分割単位の名称である「ｎｏｒｍａｌ－ＯＳ」を指定する（６１４）。論理分割制御部１４３は、「ａｃｔｉｖａｔｅ」コマンドの要求を受け付け、論理的に通常ＯＳを稼動させるために確保した計算機資源を利用可能にし、ＦＤドライブ１１２からフロッピーディスク内に格納されている起動用プログラムを読み出し、論理的に計算機資源を起動し、ＯＳのインストール作業を開始する。通常ＯＳに関する様々な情報をＣＤ－ＲＯＭドライブ１１３から読み出し、磁気ディスク装置１２１へ格納する。

【００６１】前記通常ＯＳのインストール後、システム管理者は論理分割制御部１４３に対し、通常ＯＳの起動用デバイスを、ＦＤドライブ１１２から通常ＯＳをインストールした磁気ディスク装置１２１にきりかえる（６１５）。具体的には、「ｓｅｔ」コマンドを入力装置１１０から入力し、そのコマンドの引数として、論理分割単位の名称である「ｎｏｒｍａｌ－ＯＳ」と（６１６）ＯＳ起動用の磁気ディスク装置１２１のデバイス番号「８１」を指定する（６１７）。

【００６２】次に、論理分割制御部１４３に対し、セキュアＯＳ用の計算機資源を設定する（６１８）。具体的には、「ｓｅｔ」コマンドを入力装置１１０から入力し、そのコマンドの引数として、論理分割単位の名称となる「ｓｅｃｕｒｅ－ＯＳ」と（６１９）、最初のＣＰＵ使用比率の割り当てとなる、ＣＰＵ全体の使用率に対する割合「６０」パーセント（％）と（６２０）、セキュアＯＳが使用する物理的なメモリ容量「１０２４」メガバイト（ＭＢ）と（６２１）、ＯＳ起動用のデバイスとしてＦＤを使うために、前記手順６０２で調べたＦＤドライブのデバイス番号「０１」と（６２２）、磁気ディスク装置１２２を利用するために、あらかじめ設定しておいた割り込み要求番号「０ｘ０Ｅ」を指定する（６２３）。論理分割制御部１４３は、「ｓｅｔ」コマンドの

要求を受け付け、システム管理者が要求したセキュアＯＳに割り当てる計算機資源の確保をする。

【００６３】次に、セキュアＯＳをインストールする作業をとり行うためのフロッピーディスクをＦＤドライブ１１２へ挿入し、各種セキュアＯＳに関する情報を格納してあるＣＤ－ＲＯＭをＣＤ－ＲＯＭドライブ１１３へ挿入する。

【００６４】次に、論理分割制御部１４３に対し、セキュアＯＳの計算機資源を実際に使用可能な状況にするために、「ａｃｔｉｖａｔｅ」コマンドを入力する（６２４）。具体的には、「ａｃｔｉｖａｔｅ」コマンドを入力装置１１０から入力し、そのコマンドの引数として、セキュアＯＳの論理分割単位の名称である「ｓｅｃｕｒｅ－ＯＳ」を指定する（６２５）。論理分割制御部１４３は、「ａｃｔｉｖａｔｅ」コマンドの要求を受け付け、論理的にセキュアＯＳを稼動させるために確保した計算機資源を利用可能にし、ＦＤドライブ１１２からフロッピーディスク内に格納されている起動用プログラムを読み出し、論理的に計算機資源を起動し、ＯＳのインストール作業を開始する。セキュアＯＳに関する様々な情報をＣＤ－ＲＯＭドライブ１１３から読み出し、磁気ディスク装置１２２へ格納する。

【００６５】前記セキュアＯＳのインストール後、システム管理者は論理分割制御部１４３に対し、セキュアＯＳの起動用デバイスを、ＦＤドライブ１１２からセキュアＯＳをインストールした磁気ディスク装置１２２にきりかえる（６２６）。具体的には、「ｓｅｔ」コマンドを入力装置１１０から入力し、そのコマンドの引数として、論理分割単位の名称である「ｓｅｃｕｒｅ－ＯＳ」と（６２７）ＯＳ起動用の磁気ディスク装置１２２のデバイス番号「８２」を指定する（６２８）。

【００６６】以上のコマンド入力手続き６０１～６２８＊

６０（％）　×　０．９　＝　５４（％）…… セキュアＯＳのＣＰＵ使用比率

と算出する。

【００７２】ステップ４０３で算出した新たなセキュアＯＳのＣＰＵ使用比率から、通常ＯＳのＣＰＵ使用比率※

１００（％）－　５４（％）　＝　４６（％）…… 通常ＯＳのＣＰＵ使用比率

と算出する。その後、ステップ４０７へ進む。

【００７３】一方、ＣＰＵの使用率が閾値を超えたのがセキュアＯＳだった場合、通常ＯＳの現状のＣＰＵ使用比率(本実施例では４０％)をある一定の割合で減らし　★

４０（％）　×　０．９　＝　３６（％）…… 通常ＯＳのＣＰＵ使用比率

１００（％）－　３６（％）＝　６４（％）… セキュアＯＳのＣＰＵ使用比率

と算出する。

【００７４】前記ステップ４０３～４０６で算出した新たなＣＰＵ使用比率を、入力装置１１０から、論理分割制御部１４３に対して設定する（ステップ４０７）。設定後、ステップ４１０へ進む。

【００７５】次に、システム管理者が資源利用状況計測部１６６から受信した情報を再度参照し、メモリの使用＊により、通常ＯＳとセキュアＯＳがインストールされ、各ＯＳの制御の元で、前記暗号化通信によるアクセス処理部１６３や、資源利用状況計測部１６６や、秘密鍵を用いた暗号復号処理部１５３や、資源利用状況計測部１５４が稼動する。

【００６７】次に、システム管理者が、前記資源利用状況計測部１６６から何らかの計算機資源が閾値を超えている旨を受信した場合に、計算機資源を再配分する処理手順を図４、図６を用いて説明する。

【００６８】図４に、システム管理者が資源利用状況計測部１６６から受信した情報をもとに、新たなＣＰＵ使用比率またはメモリ容量を具体的に決定し、再設定する手順を示す。

【００６９】システム管理者が資源利用状況計測部１６６から受信した情報を参照し、ＣＰＵの使用率が閾値を超えていたという通知かどうかを判断する（ステップ４０１）。ＣＰＵの使用率が閾値を超えていた場合には、手続き４０２へ進み、超えていなかった場合は、手続き４１０へ進む。

【００７０】ＣＰＵの使用率が閾値を超えていた場合には、閾値を超えたのは通常ＯＳなのか、セキュアＯＳなのか、その両方のＯＳなのかを判断する（ステップ４０２）。通常ＯＳだった場合には、手続き４０３へ進み、セキュアＯＳだった場合には、手続き４０５へ進み、両方のＯＳだった場合には、情報サーバ装置のＣＰＵ資源全体が足りないということになるため、現状のＣＰＵ使用比率の設定は変更せず、手続き４１０へ進む。

【００７１】ＣＰＵの使用率が閾値を超えたのが通常ＯＳだった場合、セキュアＯＳの現状のＣＰＵ使用比率(本実施例では６０％)をある一定の割合で減らす（ステップ４０３）。例えば、現使用比率の１割を減らす場合には、

※を算出する（ステップ４０４）。前記の例を引き続き用いると、

★（ステップ４０５）、新たな通常ＯＳのＣＰＵ使用比率から、セキュアＯＳのＣＰＵ使用比率を算出する（ステップ４０６）。例えば、現使用比率の１割を減らす場合には、

率が閾値を超えていたという通知かどうかを判断する（ステップ４１０）。メモリの使用率が閾値を超えていた場合には、手続き４１１へ進み、超えていなかった場合は、本再設定の処理を終了する（ステップ４２０）。

【００７６】メモリの使用率が閾値を超えていた場合には、本情報サーバ装置に未使用のメモリ資源が残されているかどうかを確認し（ステップ４１１）、もし残って

いれば、未使用のメモリ資源の一部または全部を、閾値を超えてしまったＯＳのメモリ資源として割り当てる（ステップ４１２）。割り当てる量については、ＣＰＵ使用率を算出したときのように一定の割合量を増やしてもよいし、必要と思われる量を増やしてもよい。例えば、セキュアＯＳのメモリ容量、１０２４MBが足りなくなり、２０４８MBの未使用のメモリ資源があった場合、セキュアＯＳに対し2倍のメモリ容量となる２０４８MBのメモリ資源を割り当てる、といった手順で算出する。その後、ステップ４１８へ進む。

【００７７】ステップ４１１で、本情報サーバ装置に未使用のメモリ資源が残されていないと判断した場合、メモリ使用率の閾値を超えたのは通常ＯＳなのか、セキュアＯＳなのか、その両方のＯＳなのかを判断する（ステ＊ップ４１３）。通常ＯＳだった場合には、手続き４１４へ進み、セキュアＯＳだった場合には、手続き４１６へ進み、両方のＯＳだった場合には、情報サーバ装置のメモリ資源全体が足りないということになるため、現状のメモリ容量の設定は変更せず、本再設定の処理を終了する（ステップ４２０）。

【００７８】メモリの使用率が閾値を超えたのが通常ＯＳだった場合、セキュアＯＳの現状のメモリ容量（本実施例では１０２４MB）をある一定の割合で減らし（ステップ４１４）、前記減らしたメモリ容量を、通常ＯＳに新たに割り当てる（ステップ４１５）。例えば、セキュアＯＳの使用量の２．５割を通常ＯＳに割り当てる場合には、

１０２４（MB）×０．７５＝７６８（MB）… セキュアOSのメモリ容量
２０４８（MB）＋（１０２４（MB）－ ７６８（MB））
＝ ２３０４（MB）… 通常ＯＳのメモリ容量

と算出する。その後、ステップ４１８へ進む。

【００７９】一方、メモリ使用率が閾値を超えたのがセキュアOSだった場合、通常OSの現状のメモリ容量（本実施例では２０４８MB）をある一定の割合で減らし（ス※※テップ４１６）、前記減らしたメモリ容量を、セキュアＯＳに新たに割り当てる（ステップ４１７）。例えば、通常OSの使用量の２．５割をセキュアOSに割り当てる場合には、

２０４８（MB）×０．７５＝ １５３６（MB）… 通常ＯＳのメモリ容量
１０２４（MB）＋（２０４８（MB）－ １５３６（MB））
＝１５３６（MB）… セキュアＯＳのメモリ容量

と算出する。

【００８０】前記ステップ４１４～４１７で算出した新たなメモリ容量を、入力装置１１０から、論理分割制御部１４３に対して設定し（ステップ４１８）、本再設定の処理を終了する（ステップ４２０）。

【００８１】図６に、前記ステップ４０７およびステップ４１１およびステップ４１８で、本情報サーバ装置の計算機資源を再設定したり、未使用のメモリ資源を確認する際の、コマンド入力画面を示す。前記コマンド入力画面に対して行う操作は、入力装置１１０を介して論理分割制御システムの論理分割制御部１４３に伝わるものとする。また、以下の実施例では、すでに通常ＯＳとセキュアＯＳ用の計算機資源を、手順６０７と、手順６１５と、手順６１８と、手順６２６で設定してある場合を例にして説明する。

【００８２】まず、論理分割制御部１４３に対して、「ｌｐａｒｓｔａｔ」コマンドを入力し（７００）、現状の情報サーバ装置の資源の論理的分割状況と、未使用のメモリ容量の一覧を画面表示装置１１１に表示させる。

【００８３】各論理分割単位を識別するための情報であり、第一の論理分割単位であることを示すラベル「ＬＰ１」と（７０１）、第一の論理分割単位の名称である「ｎｏｒｍａｌ－ＯＳ」と（７０２）、第一の論理分割単位のＣＰＵ使用比率である「４０」（%）と（７０３）、第一の論理分割単位のメモリ容量である「２０４８」（MB）と（７０４）、第一の論理分割単位で使用するＯＳ起動用のデバイスの番号である「８１」と（７０５）、第一の論理分割単位で使用する割り込み要求番号である「０ｘ０Ｃ ０ｘ０Ｄ」（７０６）を表示する。

【００８４】引き続き、第二の論理分割単位であることを示すラベル「ＬＰ２」と（７１０）、第二の論理分割単位の名称である「ｓｅｃｕｒｅ－ＯＳ」と（７１１）、第二の論理分割単位のＣＰＵ使用比率である「６０」（%）と（７１２）、第二の論理分割単位のメモリ容量である「１０４８」（MB）と（７１３）、第二の論理分割単位で使用するＯＳ起動用のデバイスの番号である「８２」と（７１４）、第二の論理分割単位で使用する割り込み要求番号である「０ｘ０Ｅ」（７１５）を表示する。

【００８５】引き続き、未使用のメモリ容量を表示するためのラベル「Ｍｅｍｏｒｙ ｄｉｓｔｒｉｂｕｔｉｏｎ」と（７２０）、通常ＯＳに割り当てられているメモリ容量を示す「ＬＰ１ ｎｏｒｍａｌ－ＯＳ ２０４８（MB）」（７２１）と、セキュアＯＳに割り当てられているメモリ容量を示す「ＬＰ２ ｓｅｃｕｒｅ－ＯＳ １０２４（MB）」（７２２）と、未使用のメモリ容量を示す「Ｒｅｍａｉｎｉｎｇ ＲＡＭ ０（MB）」（７２３）を表示する。本実施例では、未使用のメモリがない、すなわち、情報サーバ装置に備えるすべてのメモリ資源を、通常ＯＳまたはセキュアＯＳへ割り当てて

いるものとする。未使用のメモリ資源がある場合には、未使用のメモリ容量「Ｒｅｍａｉｎｉｎｇ　ＲＡＭ」欄に未使用のメモリ容量の値が表示される。

【００８６】次に、「ｌｐａｒｓｔａｔ」コマンドで情報を表示させた後、ＣＰＵ使用比率と、メモリ容量を設定する手順を示す。本実施例では、通常ＯＳのＣＰＵ使用率と通常ＯＳのメモリ使用率とが閾値を超え、セキュアＯＳのＣＰＵ使用率の１割分と、セキュアＯＳのメモリ容量の２．５割分を通常ＯＳの計算機資源として再設定する例を示す。

【００８７】まず、論理分割制御部１４３に対して、「ｓｅｔ」コマンドを用いて、通常ＯＳの計算機資源の情報を更新する（７３０）。コマンドの引数として、論理分割単位の名称である「ｎｏｒｍａｌ－ＯＳ」と（７３１）と、ＣＰＵ使用比率「４６」（％）と（７３２）、メモリ容量「２３０４」（ＭＢ）を指定する（７３３）。

【００８８】引き続き、論理分割制御部１４３に対して、「ｓｅｔ」コマンドを用いて、セキュアＯＳの計算機資源の情報を更新する（７４０）。コマンドの引数として、論理分割単位の名称である「ｓｅｃｕｒｅ－ＯＳ」と（７４１）と、ＣＰＵ使用比率「５４」（％）と（７４２）、メモリ容量「７６８」（ＭＢ）を指定する（７４３）。

【００８９】本実施例では手順７３０および手順７４０の操作を、通常ＯＳおよびセキュアＯＳが稼動している最中でも指定可能である論理分割制御システムを前提にしている。前記再設定の操作のために、稼動中のＯＳを一度停止させなければならない論理分割制御システムの場合には、以下に示す手順となる。

【００９０】手順７３０を実施する前に、通常ＯＳにて、通常ＯＳを停止させる「シャットダウン」操作を行う。次に、論理分割制御部１４３に対し、通常ＯＳの計算機資源を使用不可能な状況にするために、「ｄｅａｃｔｉｖａｔｅ」コマンドを入力し、そのコマンドの引数として、通常ＯＳの論理分割単位の名称である「ｎｏｒｍａｌ－ＯＳ」を指定する。次に手順７３０を実施し、通常ＯＳの計算機資源を使用可能な状況にするために、「ａｃｔｉｖａｔｅ」コマンドを入力し、そのコマンドの引数として、通常ＯＳの論理分割単位の名称である「ｎｏｒｍａｌ－ＯＳ」を指定する。

【００９１】同様に、手順７４０を実施する前に、セキュアＯＳにて、セキュアＯＳを停止させる「シャットダウン」操作を行う。次に、論理分割制御部１４３に対し、セキュアＯＳの計算機資源を使用不可能な状況にするために、「ｄｅａｃｔｉｖａｔｅ」コマンドを入力し、そのコマンドの引数として、セキュアＯＳの論理分割単位の名称である「ｓｅｃｕｒｅ－ＯＳ」を指定する。次に手順７４０を実施し、セキュアＯＳの計算機資源を使用可能な状況にするために、「ａｃｔｉｖａｔｅ」コマンドを入力し、そのコマンドの引数として、セキュアＯＳの論理分割単位の名称である「ｓｅｃｕｒｅ－ＯＳ」を指定する。

【００９２】なお、本実施例では、情報サーバ装置で稼動させるＯＳとして、端末装置との情報通信全般を司る通常ＯＳと、暗号処理を司るセキュアＯＳを稼動させる例を述べたが、セキュアＯＳの変わりに、別の処理を専門とするＯＳを稼動させても構わない。

【００９３】例えば、従来のＷｅｂサーバシステムでは、データベースへのアクセスを受け付け、Ｗｅｂサーバに接続するデータベースの内容に応じて、端末装置へ送付する表示内容を動的に生成する機能を備えているものもある。当該Ｗｅｂサーバでは、端末装置からの要求をデータベースに伝えるために、ＣＧＩ（Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅ）というインターフェースを用いるが、ＣＧＩを処理するプログラムがＷｅｂサーバのＣＰＵ負荷をかける原因となることが判っている。そこで、ＣＧＩ用のＯＳを稼動し、ＣＧＩ用ＯＳに対し計算機資源を割り当て、通常ＯＳからＣＧＩ用ＯＳへＣＧＩの処理を依頼する。このことで、ＣＧＩの処理により発生していたＷｅｂサーバの反応速度の低下を回避することが可能となる。

【００９４】

【発明の効果】本発明によれば、特別なアクセラレータ装置を装備しない情報サーバ装置において、少なくとも非暗号通信のアクセスに対する反応速度低下を回避することが可能となり、さらには、秘密鍵の漏洩防止が可能となる。

【図面の簡単な説明】

【図１】情報サーバ装置の構成図

【図２】情報サーバ装置における暗号処理の流れ

【図３】資源利用状況計測部の処理の流れ

【図４】ＣＰＵ使用比率とメモリ容量の決定および設定手続きの流れ

【図５】通常ＯＳとセキュアＯＳインストール時の計算機資源配分のコマンド入力画面

【図６】通常ＯＳとセキュアＯＳの計算機資源再配分のコマンド入力画面

【符号の説明】

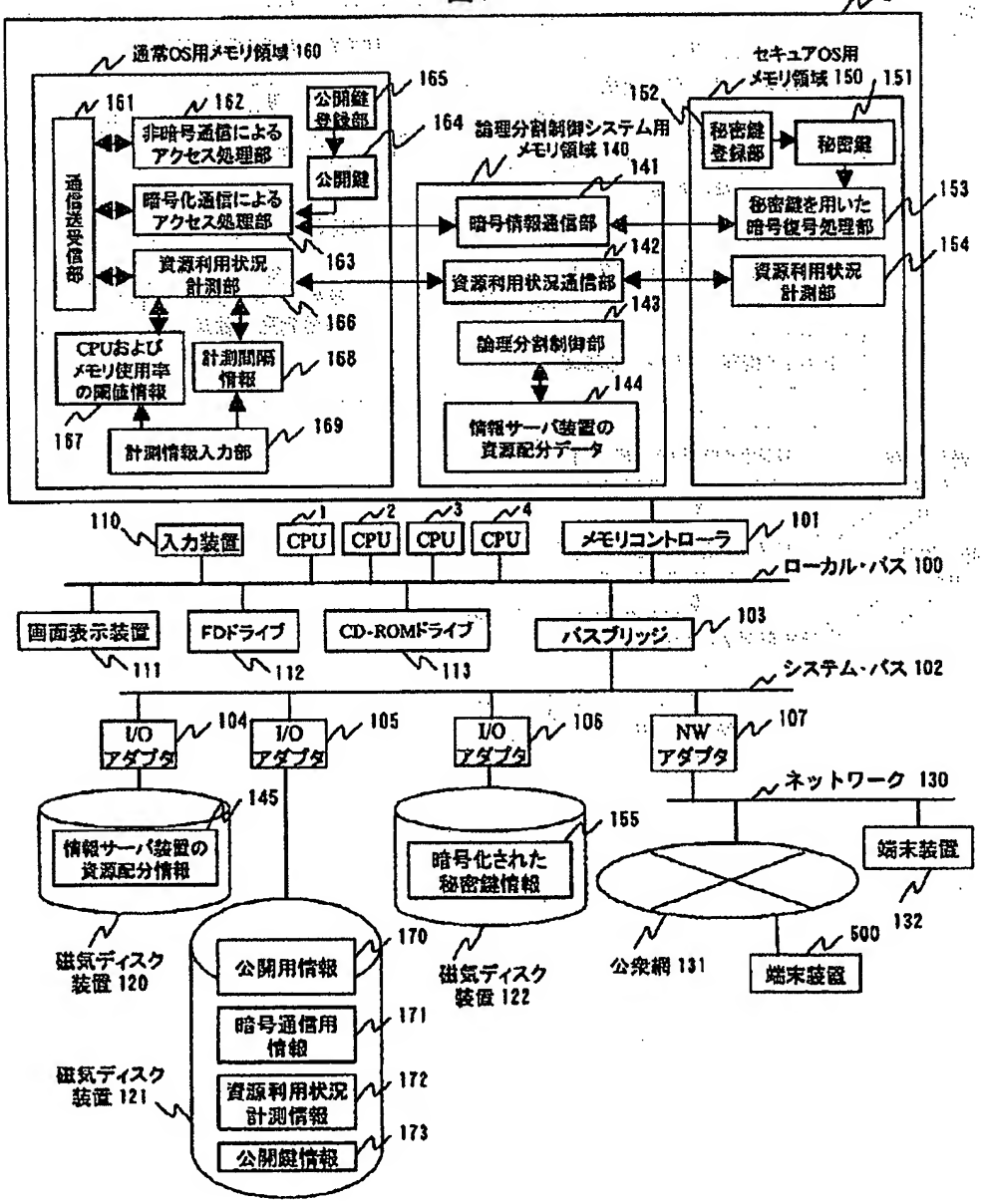
１～４…情報サーバ装置に備えるＣＰＵ
５…情報サーバ装置に備えるメモリ
１１０…情報サーバ装置に備える入力装置
１１１…情報サーバ装置に備える画面表示装置
１１２…情報サーバ装置に備えるＦＤドライブ
１１３…情報サーバ装置に備えるＣＤ－ＲＯＭドライブ
１２０…論理分割制御システム用磁気ディスク装置
１２１…通常ＯＳ用磁気ディスク装置
１２２…セキュアＯＳ用磁気ディスク装置
１３０…ネットワーク
１３１…公衆網

１３２…システム管理者が閾値を超えた旨を受信する端末装置
１４０…論理分割制御システム用メモリ領域
１４１…暗号情報通信部
１４２…資源利用状況通信部
１４３…論理分割制御部
１５０…セキュアＯＳ用メモリ領域
１５１…秘密鍵
１５２…秘密鍵登録部
１５３…秘密鍵を用いた暗号復号処理部
＊１５４…セキュアＯＳの資源利用状況計測部
１６０…通常ＯＳ用メモリ領域
１６１…通信送受信部
１６２…非暗号通信によるアクセス処理部
１６３…暗号通信によるアクセス処理部
１６４…公開鍵
１６５…公開鍵登録部
１６６…通常ＯＳの資源利用状況計測部
５００…情報サーバ装置にアクセスする端末装置

＊10

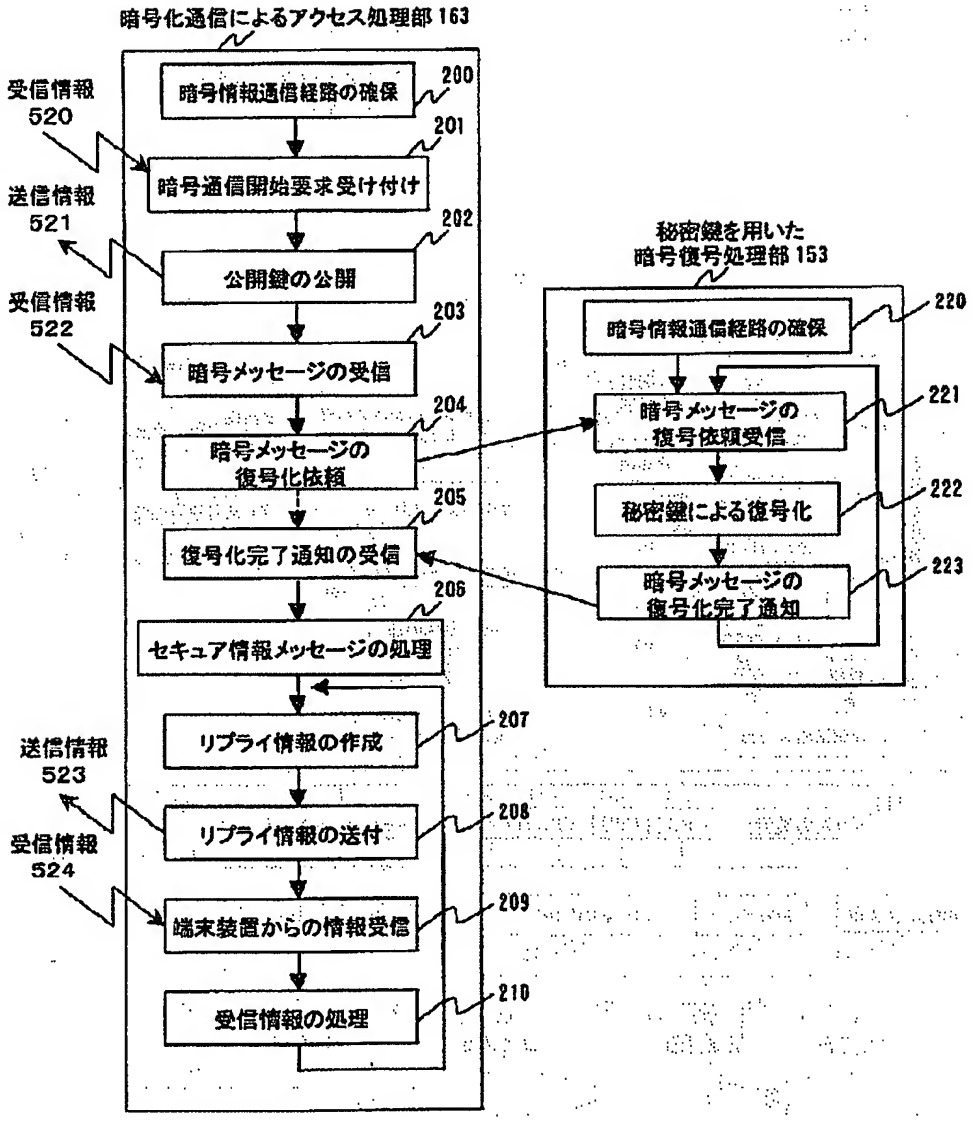
【図１】

図1



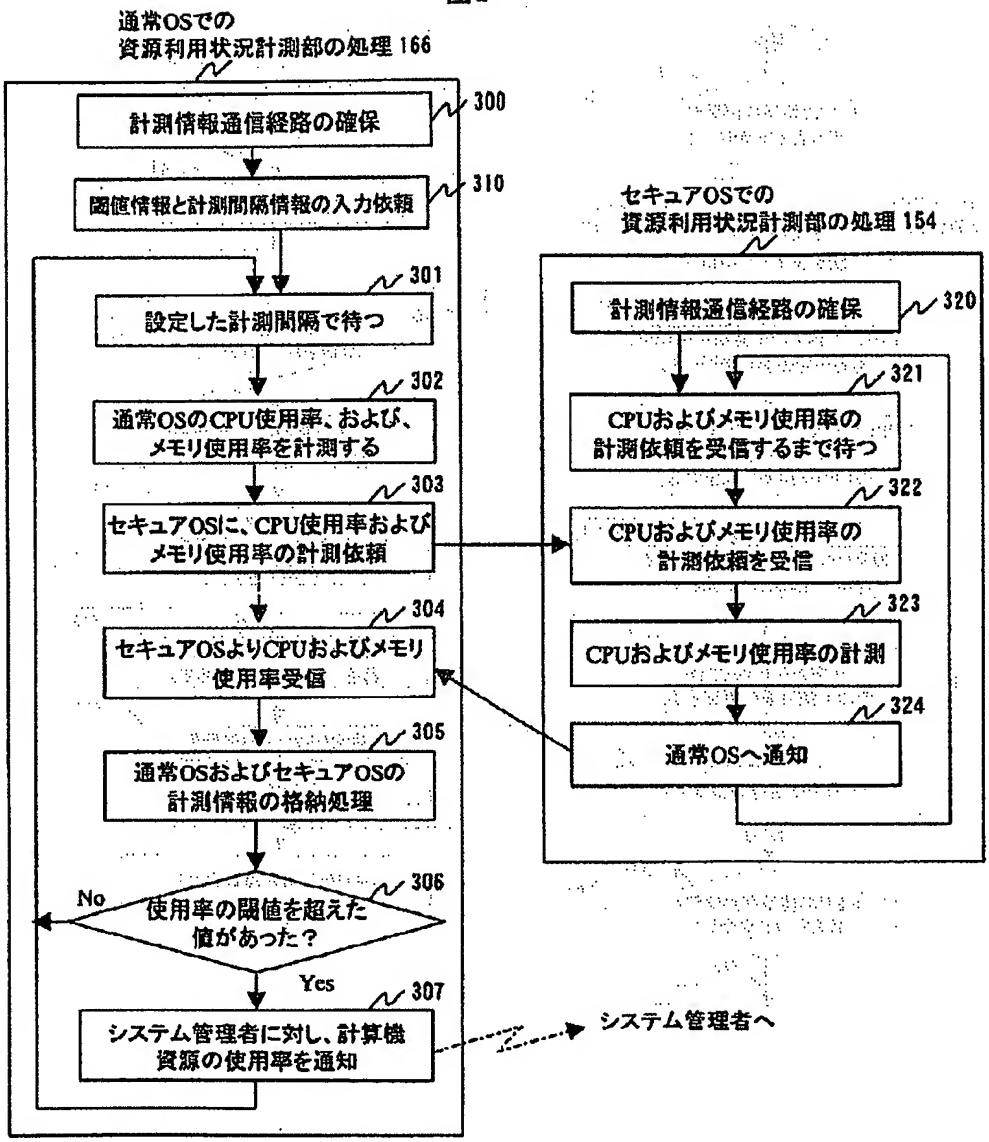
【図２】

図2


暗号化通信によるアクセス処理部 163
暗号情報通信経路の確保
200
受信情報
520
暗号通信開始要求受け付け
201
送信情報
521
公開鍵の公開
202
受信情報
522
暗号メッセージの受信
203
暗号メッセージの
復号化依頼
204
復号化完了通知の受信
205
セキュア情報メッセージの処理
206
リプライ情報の作成
207
送信情報
523
リプライ情報の送付
208
受信情報
524
端末装置からの情報受信
209
受信情報の処理
210
秘密鍵を用いた
暗号復号処理部 153
暗号情報通信経路の確保
220
暗号メッセージの
復号依頼受信
221
秘密鍵による復号化
222
暗号メッセージの
復号化完了通知
223

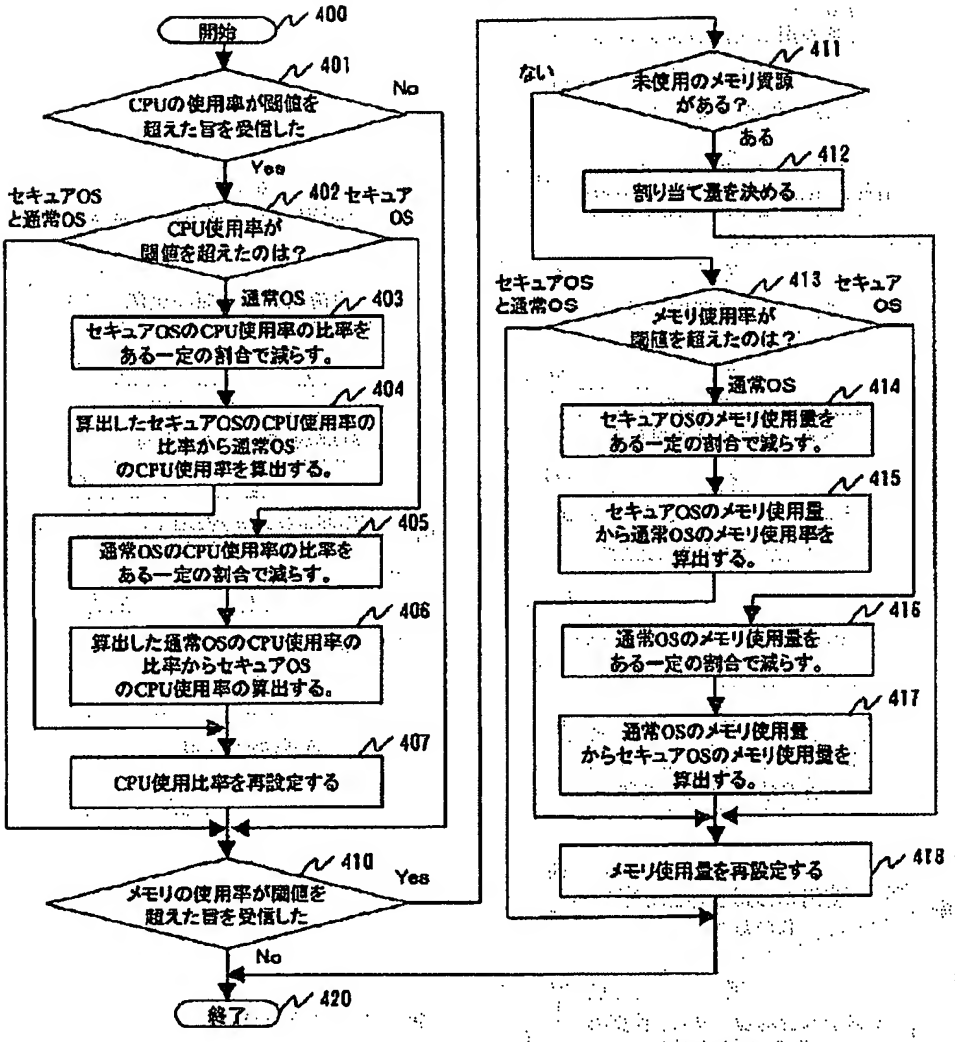
【図３】

図3


通常OSでの
資源利用状況計測部の処理 166
計測情報通信経路の確保
300
閾値情報と計測間隔情報の入力依頼
310
設定した計測間隔で待つ
301
通常OSのCPU使用率、および、
メモリ使用率を計測する
302
セキュアOSに、CPU使用率および
メモリ使用率の計測依頼
303
セキュアOSよりCPUおよびメモリ
使用率受信
304
通常OSおよびセキュアOSの
計測情報の格納処理
305
使用率の閾値を超えた
値があった？
306
No
Yes
システム管理者に対し、計算機
資源の使用率を通知
307
システム管理者へ
セキュアOSでの
資源利用状況計測部の処理 154
計測情報通信経路の確保
320
CPUおよびメモリ使用率の
計測依頼を受信するまで待つ
321
CPUおよびメモリ使用率の
計測依頼を受信
322
CPUおよびメモリ使用率の計測
323
通常OSへ通知
324

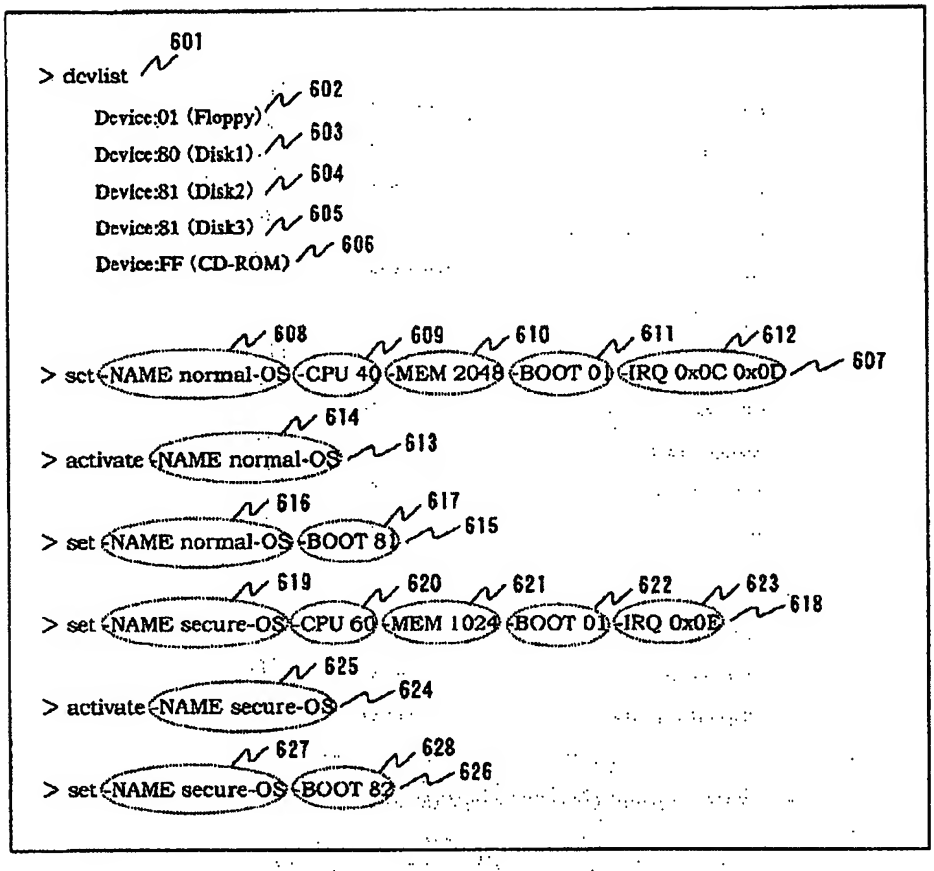
【図４】

図4


開始
400
CPUの使用率が閾値を超えた旨を受信した
401
No
Yes
セキュアOSと通常OS
CPU使用率が閾値を超えたのは？
402
セキュアOS
通常OS
セキュアOSのCPU使用率の比率をある一定の割合で減らす。
403
算出したセキュアOSのCPU使用率の比率から通常OSのCPU使用率を算出する。
404
通常OSのCPU使用率の比率をある一定の割合で減らす。
405
算出した通常OSのCPU使用率の比率からセキュアOSのCPU使用率の算出する。
406
CPU使用比率を再設定する
407
メモリの使用率が閾値を超えた旨を受信した
410
Yes
No
終了
420
ない
未使用のメモリ資源がある？
411
ある
割り当て量を決める
412
セキュアOSと通常OS
メモリ使用率が閾値を超えたのは？
413
セキュアOS
通常OS
セキュアOSのメモリ使用量をある一定の割合で減らす。
414
セキュアOSのメモリ使用量から通常OSのメモリ使用率を算出する。
415
通常OSのメモリ使用量をある一定の割合で減らす。
416
通常OSのメモリ使用量からセキュアOSのメモリ使用量を算出する。
417
メモリ使用量を再設定する
418

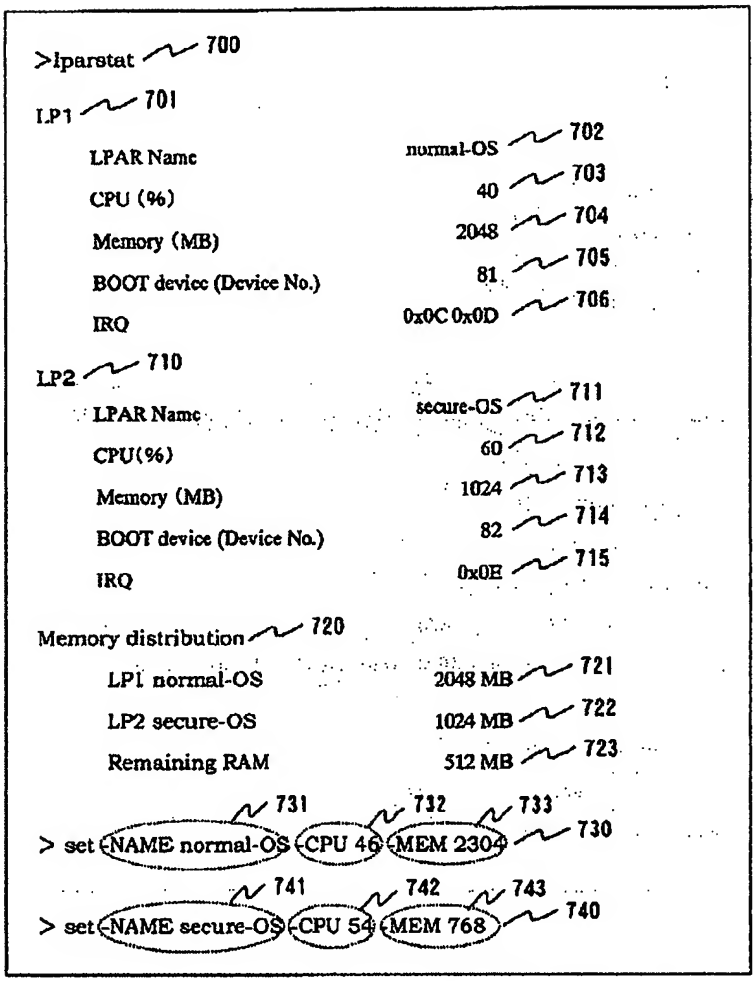
【図５】

図5


601
> devlist
Device:01 (Floppy)
602
Device:80 (Disk1)
603
Device:81 (Disk2)
604
Device:81 (Disk3)
605
Device:FF (CD-ROM)
606
608
609
610
611
612
> set -NAME normal-OS -CPU 40 -MEM 2048 -BOOT 0 -IRQ 0x0C 0x0D
607
614
> activate -NAME normal-OS
613
616
617
> set -NAME normal-OS -BOOT 8
615
619
620
621
622
623
> set -NAME secure-OS -CPU 60 -MEM 1024 -BOOT 01 -IRQ 0x0E
618
625
> activate -NAME secure-OS
624
627
628
> set -NAME secure-OS -BOOT 82
626

【図６】

図6




---

フロントページの続き

Ｆターム(参考) 5B085 AE29 BG07
5B098 AA10 GC10 GD02 GD03
5J104 AA01 AA16 AA17 EA04 EA19
PA07